PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2005-128922
(43)Date of publication of application : 19.05.2005

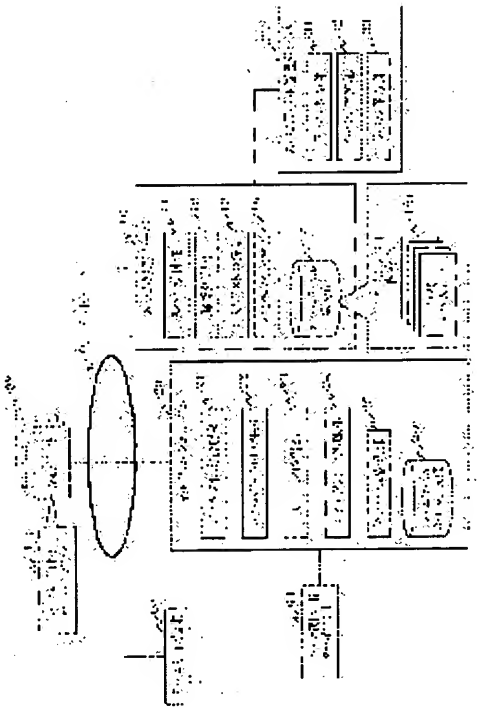
(51)Int.Cl. G06F 13/00
H04L 12/58

(21)Application number : 2003-365887
(22)Date of filing : 27.10.2003

(71)Applicant : NEC SOFTWARE KYUSHU LTD
(72)Inventor : UEDA KENJI

(54) SPAM MAIL FILTERING SYSTEM AND METHOD AND ITS PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a spam mail filtering system capable of holding a URI showing the resource of a Web site included in a spam mail, and filtering a spam mail based on the held URL at the time of referring the resource.
SOLUTION: This spam mail filtering system is provided with: a Web site where an information resource including a Web page exists; a spam issuing terminal which issues a spam mail by referring to a mail address for accepting a spam registered in an arbitrary Web site in the Web site; a spam processing server which accepts the spam mail, and stores it as a URI spam list; a spam label management server which conforms URI included in the spam mail, and corrects any error; a client for resource browsing which allows a user to perform access to an information resource; and a filtering engine which executes the filtering of browsing based on a status preliminarily set by the URI spam list from the spam processing server at the time of executing the resource browsing of URI from the client for resource browsing.



(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-128922
(P2005-128922A)
(43)公開日　平成17年5月19日(2005.5.19)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 13/00	G06F 13/00	610Q	5K030
H04L 12/58	G06F 13/00	610S	
	H04L 12/58	100F	

審査請求 有　請求項の数 14　OL　（全 17 頁）

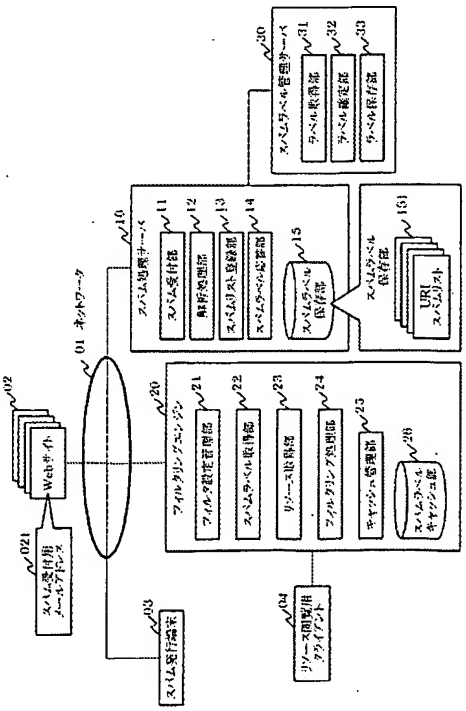
(21)出願番号　特願2003-365887 (P2003-365887)
(22)出願日　平成15年10月27日 (2003.10.27)

(71)出願人　000164449
九州日本電気ソフトウェア株式会社
福岡市早良区百道浜２丁目４－１　ＮＥＣ九州システムセンター
(74)代理人　100109313
弁理士　机　昌彦
(74)代理人　100085268
弁理士　河合　信明
(74)代理人　100111637
弁理士　谷澤　靖久
(72)発明者　上田　健次
福岡県福岡市早良区百道浜二丁目４番１号　九州日本電気ソフトウェア株式会社内

Ｆターム(参考)　5K030 GA15 HA06 HC01 HD03 KA05 LB05 MA04

(54)【発明の名称】スパムメールフィルタリングシステム，方法，およびプログラム

(57)【要約】
【課題】スパムメールに含まれるＷｅｂサイトのリソースを指すＵＲＩを保持しておき、上記のリソースを参照する場合に、保持しているＵＲＩに基づいてフィルタリングする。
【解決手段】Ｗｅｂページを含む情報リソースが存在するＷｅｂサイトと、前記Ｗｅｂサイトの中の任意のＷｅｂサイトに登録されたスパム受付用メールアドレスを参照しスパムメールを発行するスパム発行端末と、前記スパムメールを受け付けてＵＲＩスパムリストとして保持するスパム処理サーバと、前記スパムメールに含まれるＵＲＩを確認し誤りがあれば訂正するスパムラベル管理サーバと、利用者が情報リソースにアクセスするリソース閲覧用クライアントと、前記リソース閲覧用クライアントからのＵＲＩのリソース閲覧の際に前記スパム処理サーバからのＵＲＩスパムリストによって，あらかじめ設定した状態に基づいて閲覧をフィルタリングするフィルタリングエンジンとを有する。
【選択図】　図1



【特許請求の範囲】
【請求項1】
Ｗｅｂページを含む情報リソースが存在するＷｅｂサイトと、前記Ｗｅｂサイトの中の任意のＷｅｂサイトに登録されたスパム受付用メールアドレスを参照しスパムメールを発行するスパム発行端末と、前記スパムメールを受け付けてＵＲＩスパムリストとして保持するスパム処理サーバと、前記スパムメールに含まれるＵＲＩを取得して確認し誤りがあれば訂正するスパムラベル管理サーバと、情報リソースにアクセスするためのリソース閲覧用クライアントと、前記リソース閲覧用クライアントからのＵＲＩのリソース閲覧の際に前記スパム処理サーバからのＵＲＩスパムリストによって，あらかじめ設定した状態に基づいて閲覧をフィルタリングするフィルタリングエンジンと、前記Ｗｅｂサイト，前記スパム発行端末，前記スパム処理サーバ，および前記フィルタリングエンジンを相互に接続するネットワークとを有することを特徴とするスパムメールフィルタリングシステム。
【請求項2】
前記スパム処理サーバは、スパムメールを受け付けるスパム受付部と、前記スパムメールの内容を解析する解析処理部と、前記スパムメール内のＵＲＩをＵＲＩスパムリストとして登録するスパムリスト登録部と、前記ＵＲＩスパムリストを保存するスパムラベル保存部と、前記スパムラベル保存部のＵＲＩスパムリストの問合せによって応答を行うスパムラベル応答部とを具備することを特徴とする請求項1記載のスパムメールフィルタリングシステム。
【請求項3】
前記スパムラベル管理サーバは、前記スパム処理サーバからＵＲＩスパムリストを取得するラベル取得部と、ＵＲＩのリソースを取得して表示し当該リソースが有害か否かを確定するラベル確定部と、確定したＵＲＩを前記スパム処理サーバに送付して前記スパムラベル保存部の更新を指示するラベル保存部とを具備することを特徴とする請求項1または2記載のスパムメールフィルタリングシステム。
【請求項4】
前記フィルタリングエンジンは、前記ＵＲＩスパムリストによってフィルタリングを行うか否かを含めてフィルタリング条件を設定するフィルタ設定管理部と、前記リソース閲覧用クライアントからのＵＲＩ参照要求の際に前記スパム処理サーバからＵＲＩスパムリストを取得するスパムラベル取得部と、前記フィルタ設定管理部が設定したフィルタリング条件と前記スパムラベル取得部が取得したＵＲＩスパムリストとによってフィルタリングを行うフィルタリング処理部と、フィルタリング不要あるいは閲覧可能の場合に当該ＵＲＩのリソースを取得しそれを前記リソース閲覧用クライアントに送付するリソース取得部とを具備することを特徴とする請求項1，２，または３記載のスパムメールフィルタリングシステム。
【請求項5】
前記フィルタリングエンジンは、前記スパムラベル取得部が取得したＵＲＩスパムリストをキャッシュとして保存するスパムラベルキャッシュ部およびそれを制御するキャッシュ管理部を備え、前記リソース閲覧用クライアントからのＵＲＩ参照要求の際に当該ＵＲＩを既に取得しているか否か前記スパムラベルキャッシュ部をチェックし、取得済みの場合にはそれを参照することを特徴とする請求項４記載のスパムメールフィルタリングシステム。
【請求項6】
前記スパム処理サーバは、あらかじめキーワードを登録しているキーワード保存部と、前記解析処理部がスパムメールを解析する際に前記スパムメールに含まれるキーワードを抽出し，それを前記キーワード保存部のキーワードと比較して当該キーワードの有害度を判断し，前記スパムメールを格付けするスパムラベル格付部と、前記スパムラベル格付部の格付結果に基づいて当該ＵＲＩおよびそのスパムラベルをスパムラベル保存部に登録するスパムラベル登録部とを備えることを特徴とする請求項２記載のスパムメールフィルタ

リングシステム。

【請求項7】

前記Ｗｅｂサイトにスパムメールを受信可能な複数のメールアドレスを有しそれぞれのメールアドレスに同一のスパムメールを受信し、前記複数のメールアドレスの一つが受信したスパムメールを受付けてそれを前記スパム処理サーバへ送付する第二スパム処理サーバを備え、前記スパム処理サーバでは自身が受付けたスパムメールと前記第二スパム処理サーバから送付されたスパムメールとが同一のスパムメールであることを認識して解析処理することを特徴とする請求項１または２記載のスパムメールフィルタリングシステム。

【請求項8】

前記スパム処理サーバは、前記複数のメールアドレスの一つが受信した第一のスパムメールと前記複数のメールアドレスの他の一つが受信した第二のスパムメールとを比較し両者が同一のスパムメールであることを認識する際、それぞれのメールの内容を突き合せて照合し同じ内容を含む照合率に基づいて判定することを特徴とする請求項１，２，または７記載のスパムメールフィルタリングシステム。

【請求項9】

スパムメールを受け付け、前記スパムメール内に含まれるＵＲＩを収集しそれをＵＲＩスパムリストとして保持し、フィルタリングを行う際には、前記ＵＲＩスパムリストを参照し、あらかじめ設定されているフィルタリング条件に基づいてフィルタリングすることを特徴とするスパムメールフィルタリング方法。

【請求項10】

スパムメールを解析する際に前記スパムメールに含まれるキーワードを抽出し、それをあらかじめ登録してあるキーワードと比較して当該キーワードの有害度を判断し、それをスパムラベルとして前記スパムメールを格付けし、その格付結果に基づいて当該ＵＲＩおよびそのスパムラベルを保持し、フィルタリングを行う際には、前記ＵＲＩおよびそのスパムラベルを参照し、あらかじめ設定されているフィルタリング条件に基づいてフィルタリングすることを特徴とするスパムメールフィルタリング方法。

【請求項11】

複数のメールアドレスの一つが受信した第一のスパムメールと前記複数のメールアドレスの他の一つが受信した第二のスパムメールとを比較し両者が同一のスパムメールであることを認識する際、それぞれのメールの内容を突き合せて照合し同じ内容を含む照合率に基づいて判定し、その判定結果を当該ＵＲＩスパムリストに反映させることを特徴とする請求項９記載のスパムメールフィルタリング方法。

【請求項12】

スパムメールを利用して情報のフィルタリングを行う際に、スパムメールを受け付けるスパム受付機能と、前記スパムメールの内容を解析する解析処理機能と、前記スパムメール内のＵＲＩをＵＲＩスパムリストとして登録するスパムリスト登録機能と、前記ＵＲＩスパムリストを保存するスパムラベル保存機能と、前記ＵＲＩスパムリストへの問合せによって応答を行うスパムラベル応答機能とを、コンピュータに実現させるためのスパムメールフィルタリングプログラム。

【請求項13】

前記ＵＲＩスパムリストによってフィルタリングを行うか否かを含めてフィルタリング条件を設定するフィルタ設定管理機能と、リソース閲覧用クライアントからのＵＲＩ参照要求の際に前記ＵＲＩスパムリストを取得するスパムラベル取得機能と、前記フィルタ設定管理機能が設定したフィルタリング条件と前記スパムラベル取得機能が取得したＵＲＩスパムリストとによってフィルタリングを行うフィルタリング処理機能と、フィルタリング不要あるいは閲覧可能の場合に当該ＵＲＩのリソースを取得しそれを前記リソース閲覧用クライアントに送付するリソース取得機能とを、コンピュータに実現させるための請求項１２記載のスパムメールフィルタリングプログラム。

【請求項14】

スパムメールを解析する際に前記スパムメールに含まれるキーワードを抽出し、それを

あらかじめ登録してあるキーワードと比較して当該キーワードの有害度を判断し、それをスパムラベルとして前記スパムメールを格付けし、その格付結果に基づいて当該ＵＲＩおよびそのスパムラベルを保持し、フィルタリングを行う際には、前記ＵＲＩおよびそのスパムラベルを参照し、あらかじめ設定されているフィルタリング条件に基づいてフィルタリングする機能を、コンピュータに実現させるためのスパムメールフィルタリングプログ

【発明の詳細な説明】

【技術分野】

【0001】

本発明はスパムメールフィルタリングシステム，方法，およびプログラムに関し、特にスパムメールを利用して情報のフィルタリングを制御するスパムメールフィルタリングシステム，方法，およびプログラムに関する。

【背景技術】

【0002】

従来、有害なＷｅｂサイトのリソース（スパムまたはスパムメールという。）閲覧をフィルタリングする手法としては、インターネット上の情報にメタデータラベルを付与して、これをもとにフィルタリングする手法がある。メタデータラベルの付与には、情報発信者自らが付与するセルフレイティングの手法と、第三者が付与する手法がある。

【0003】

あるいはこのほか、情報に含まれる有害なキーワードや画像のイメージマッチングなどの照合処理によって、メタデータラベルを用いずにフィルタリングする手法もある。

【0004】

しかし、セルフレイティングの手法は、情報発信者が付与する手間や付与しても利用されない，あるいは不特定多数に閲覧させるために意図的に付与しない，などの理由から、普及していない。

【0005】

さらに、第三者レイティングの手法では、世界中の不特定多数の人が作成する情報は爆発的に増大していることから、新規に作成された情報やＵＲＩ（ｕｎｉｆｏｒｍ　ｒｅｓｏｕｒｃｅ　ｉｄｅｎｔｉｆｉｅｒの略。）が変更された情報にはメタデータラベルの付与が間に合わなかったり、あるいは膨大な費用を投じてメタデータラベルを付与する必要がある。あるいは、格付けには時間がかかることから、スパムメールが出回った直後にその情報が閲覧されてしまったあと、格付け結果が反映されるという状態になっており、期間限定の違法な情報を掲載したようなＷｅｂサイトのＵＲＩを含むスパムメールに対しては有効なフィルタリング手段ではない。

【0006】

キーワードやイメージマッチングなどの照合方式では、有効な情報まで誤ってフィルタリングされたり、あるいは有効な情報の検索さえできないといったマイナス面が発生することもある。

【0007】

上記のように、スパムメールに対する有効なフィルタリング手法は見出されていないが、最近ではスパムの発信源を発見した場合にはそれが発行する全電子メールの配信サービスをブロックするなどが提案されている（たとえば、特許文献１参照。）

【特許文献1】特表２００１－５２７２５７号公報（第９～１３頁，図１）

【発明の開示】

【発明が解決しようとする課題】

【0008】

上述のように、従来の情報フィルタリング方法では、個別情報に対する適切な格付けをタイムリーに取得し、それをフィルタリングに反映させることは困難である。また、発信源データに基づいて電子メールの配信を制御することにより、スパムメールなどの受信をブロックさせる手法もあるが、これは情報の内容を評価してフィルタリングしていることにはならない。すなわち、貴重な情報がスパムメールとして配信されない恐れもある。

【0009】
本発明の目的は、上記のような欠点を改善するために、スパムメールに含まれるＷｅｂサイトのリソースを指すＵＲＩを保持しておき、利用者がこのＵＲＩのリソースを参照する場合に、保持しているＵＲＩに基づいてフィルタリングするスパムメールフィルタリングシステム，方法，およびプログラムを提供することにある。
【課題を解決するための手段】
【0010】
本発明のスパムメールフィルタリングシステムは、Ｗｅｂページを含む情報リソースが存在するＷｅｂサイトと、前記Ｗｅｂサイトの中の任意のＷｅｂサイトに登録されたスパム受付用メールアドレスを参照しスパムメールを発行するスパム発行端末と、前記スパムメールを受け付けてＵＲＩスパムリストとして保持するスパム処理サーバと、前記スパムメールに含まれるＵＲＩを取得して確認し誤りがあれば訂正するスパムラベル管理サーバと、情報リソースにアクセスするためのリソース閲覧用クライアントと、前記リソース閲覧用クライアントからのＵＲＩのリソース閲覧の際に前記スパム処理サーバからのＵＲＩスパムリストによって，あらかじめ設定した状態に基づいて閲覧をフィルタリングするフィルタリングエンジンと、前記Ｗｅｂサイト，前記スパム発行端末，前記スパム処理サーバ，および前記フィルタリングエンジンを相互に接続するネットワークとを有することを特徴とする。
【0011】
さらに、本発明において、前記スパム処理サーバは、スパムメールを受け付けるスパム受付部と、前記スパムメールの内容を解析する解析処理部と、前記スパムメール内のＵＲＩをＵＲＩスパムリストとして登録するスパムリスト登録部と、前記ＵＲＩスパムリストを保存するスパムラベル保存部と、前記スパムラベル保存部のＵＲＩスパムリストの問合せによって応答を行うスパムラベル応答部とを具備することを特徴とする。
【0012】
さらに、本発明において、前記スパムラベル管理サーバは、前記スパム処理サーバからＵＲＩスパムリストを取得するラベル取得部と、ＵＲＩのリソースを取得して表示し当該リソースが有害か否かを確定するラベル確定部と、確定したＵＲＩを前記スパム処理サーバに送付して前記スパムラベル保存部の更新を指示するラベル保存部とを具備することを特徴とする。
【0013】
さらに、本発明において、前記フィルタリングエンジンは、前記ＵＲＩスパムリストによってフィルタリングを行うか否かを含めてフィルタリング条件を設定するフィルタ設定管理部と、前記リソース閲覧用クライアントからのＵＲＩ参照要求の際に前記スパム処理サーバからＵＲＩスパムリストを取得するスパムラベル取得部と、前記フィルタ設定管理部が設定したフィルタリング条件と前記スパムラベル取得部が取得したＵＲＩスパムリストとによってフィルタリングを行うフィルタリング処理部と、フィルタリング不要あるいは閲覧可能の場合に当該ＵＲＩのリソースを取得しそれを前記リソース閲覧用クライアントに送付するリソース取得部とを具備することを特徴とする。
【0014】
さらに、本発明において、前記フィルタリングエンジンは、前記スパムラベル取得部が取得したＵＲＩスパムリストをキャッシュとして保存するスパムラベルキャッシュ部およびそれを制御するキャッシュ管理部を備え、前記リソース閲覧用クライアントからのＵＲＩ参照要求の際に当該ＵＲＩを既に取得しているか否か前記スパムラベルキャッシュ部をチェックし、取得済みの場合にはそれを参照することを特徴とする。
【0015】
さらに、本発明において、前記スパム処理サーバは、あらかじめキーワードを登録しているキーワード保存部と、前記解析処理部がスパムメールを解析する際に前記スパムメールに含まれるキーワードを抽出し，それを前記キーワード保存部のキーワードと比較して当該キーワードの有害度を判断し，前記スパムメールを格付けするスパムラベル格付部と

、前記スパムラベル格付部の格付結果に基づいて当該ＵＲＩおよびそのスパムラベルをスパムラベル保存部に登録するスパムラベル登録部とを備えることを特徴とする。

【0016】

さらに、本発明のスパムメールフィルタリングシステムは、前記Ｗｅｂサイトにスパムメールを受信可能な複数のメールアドレスを有しそれぞれのメールアドレスに同一のスパムメールを受信し、前記複数のメールアドレスの一つが受信したスパムメールを受付けてそれを前記スパム処理サーバへ送付する第二スパム処理サーバを備え、前記スパム処理サーバでは自身が受付けたスパムメールと前記第二スパム処理サーバから送付されたスパムメールとが同一のスパムメールであることを認識して解析処理することを特徴とする。

【0017】

さらに、本発明において、前記スパム処理サーバは、前記複数のメールアドレスの一つが受信した第一のスパムメールと前記複数のメールアドレスの他の一つが受信した第二のスパムメールとを比較し両者が同一のスパムメールであることを認識する際、それぞれのメールの内容を突き合せて照合し同じ内容を含む照合率に基づいて判定することを特徴とする。

【0018】

また、本発明のスパムメールフィルタリング方法は、スパムメールを受け付け、前記スパムメール内に含まれるＵＲＩを収集しそれをＵＲＩスパムリストとして保持し、フィルタリングを行う際には、前記ＵＲＩスパムリストを参照し、あらかじめ設定されているフィルタリング条件に基づいてフィルタリングすることを特徴とする。

【0019】

さらに、本発明の方法は、スパムメールを解析する際に前記スパムメールに含まれるキーワードを抽出し、それをあらかじめ登録してあるキーワードと比較して当該キーワードの有害度を判断し、それをスパムラベルとして前記スパムメールを格付けし、その格付結果に基づいて当該ＵＲＩおよびそのスパムラベルを保持し、フィルタリングを行う際には、前記ＵＲＩおよびそのスパムラベルを参照し、あらかじめ設定されているフィルタリング条件に基づいてフィルタリングすることを特徴とする。

【0020】

さらに、本発明の方法は、複数のメールアドレスの一つが受信した第一のスパムメールと前記複数のメールアドレスの他の一つが受信した第二のスパムメールとを比較し両者が同一のスパムメールであることを認識する際、それぞれのメールの内容を突き合せて照合し同じ内容を含む照合率に基づいて判定し、その判定結果を当該ＵＲＩスパムリストに反映させることを特徴とする。

【0021】

また、本発明のスパムメールフィルタリングプログラムは、スパムメールを利用して情報のフィルタリングを行う際に、スパムメールを受け付けるスパム受付機能と、前記スパムメールの内容を解析する解析処理機能と、前記スパムメール内のＵＲＩをＵＲＩスパムリストとして登録するスパムリスト登録機能と、前記ＵＲＩスパムリストを保存するスパムラベル保存機能と、前記ＵＲＩスパムリストへの問合せによって応答を行うスパムラベル応答機能とを、コンピュータに実現させることを特徴とする。

【0022】

さらに、本発明のプログラムは、前記ＵＲＩスパムリストによってフィルタリングを行うか否かを含めてフィルタリング条件を設定するフィルタ設定管理機能と、リソース閲覧用クライアントからのＵＲＩ参照要求の際に前記ＵＲＩスパムリストを取得するスパムラベル取得機能と、前記フィルタ設定管理機能が設定したフィルタリング条件と前記スパムラベル取得機能が取得したＵＲＩスパムリストとによってフィルタリングを行うフィルタリング処理機能と、フィルタリング不要あるいは閲覧可能の場合に当該ＵＲＩのリソースを取得しそれを前記リソース閲覧用クライアントに送付するリソース取得機能とを、コンピュータに実現させることを特徴とする。

【0023】

さらに、本発明のプログラムは、スパムメールを解析する際に前記スパムメールに含まれるキーワードを抽出し、それをあらかじめ登録してあるキーワードと比較して当該キーワードの有害度を判断し、それをスパムラベルとして前記スパムメールを格付けし、その格付結果に基づいて当該ＵＲＩおよびそのスパムラベルを保持し、フィルタリングを行う際には、前記ＵＲＩおよびそのスパムラベルを参照し、あらかじめ設定されているフィルタリング条件に基づいてフィルタリングする機能を、コンピュータに実現させることを特徴とする。

【0024】

すなわち、本発明は、大規模電子ジャンクメール（以後、スパム）メーリングリストを利用した不特定多数への情報発信により、たとえば子供に望ましくない情報が掲載されているＷｅｂサイトの案内が配布され、閲覧されることを防止する。

【0025】

具体的には、インターネットのＷｅｂサイトにスパム受付用のダミーのメールアドレスを用意しておき、スパム発行者がこのメールアドレス宛てに送付したスパムメールに含まれるＷｅｂサイトのリソースを指すＵＲＩを保持し、モバイル環境やパソコンなどのＷｅｂブラウザ（リソース閲覧用クライアント）からこのスパムメールに含まれるＵＲＩのリソースを参照する場合に、保持したＵＲＩに基づいてフィルタリングする。

【発明の効果】

【0026】

以上、詳細に説明したように、本発明によれば、次の効果が得られる。

【0027】

第一の効果は、スパムメールが発行されるとすぐに当該メール内のＵＲＩはフィルタリングの対象となるため、即時性の効果があることである。従来は検索エンジンなどで検索したＵＲＩを格付けしていたため、たとえば１日だけ公開している違法な情報ページを含むＵＲＩのスパムメールについては、フィルタリングシステムは対応することができなかったことが、本発明により大きく改善される。

【0028】

第二の効果は、データの収集がスパムメールによる受動的、かつ自動の収集方法になることから、運用コストを大幅に削減できることがあげられる。従来のように、ＵＲＩごとに格付けを行ったメタデータラベルを元にフィルタリングする手法では、そのラベル構築に人件費やサーバ運用費を含む膨大な費用がかかっていたが、本発明においてはサーバ運用費のみで実現可能であり、トータルコストを大幅に削減できる。

【0029】

第三の効果は、スパムメール発行者にとって、本発明が実現されることにより、スパムメール発行の価値がなくなり、スパムメールの発行そのものを抑制することができる。

【発明を実施するための最良の形態】

【0030】

以下、本発明につて図面を参照しながら説明する。

【0031】

図１は本発明の実施の第一の形態を示す構成図である。同図において、本発明によるスパムメールフィルタリングシステムは、ネットワーク０１と、Ｗｅｂページなどのリソースが存在するＷｅｂサイト０２と、Ｗｅｂサイト０２の中の任意のＷｅｂサイトに登録されたスパム受付用メールアドレス０２１と、このスパム受付用メールアドレス０２１を参照しスパムメールを発行するスパム発行端末０３と、そのスパムメールを受け付けてＵＲＩスパムリスト１５１として自動的に保持するスパム処理サーバ１０と、このスパムメールに含まれるＵＲＩを確認し誤りがあれば訂正するためのスパムラベル管理サーバ３０と、リソース閲覧用クライアント０４からのＵＲＩのリソース閲覧の際にスパム処理サーバ１０からのＵＲＩスパムリストによって，あらかじめ設定した状態によって閲覧をフィルタリングするフィルタリングエンジン２０とから構成されている。

【0032】

スパム処理サーバ１０は、スパムメールを受けつけるスパム受付部１１と、スパムメールの内容を解析する解析処理部１２と、スパムメール内のＵＲＩをＵＲＩスパムリストとして登録するスパムリスト登録部１３と、ＵＲＩスパムリスト１５１を保存したスパムラベル保存部１５と、このスパムラベル保存部１５のＵＲＩスパムリスト１５１への問い合わせによって応答を行うスパムラベル応答部１４とから構成されている。

【0033】

ここで、スパムラベル応答部１４は問い合わせによってＵＲＩスパムリスト１５１そのものを返却してもよいし、存在有無のみを返却するものでもよい。また、ＵＲＩスパムリスト１５１はＵＲＩのリストでもよいし、ＵＲＩスパムリスト１５１を識別する加工値（ハッシュなど）であってもよい。

【0034】

また、解析処理部１２が抽出するＷｅｂサイトのリソースを指すＵＲＩはスパムメールに含まれる１つある場合と複数ある場合、あるいはＵＲＩが存在しない場合もある。

【0035】

さらに、解析処理部１２においては、当該メールがスパムメールか否かを自ら判断する処理を行うケースもある。具体的には、″＿″文字で単語をつなげるパターン認識（Ｔｈｉｓ＿ｉｓ＿ａ＿ｓｐａｍ＿ｍａｉｌ）や、有害な文字に空白を含めるケース（ＭａｋｅＭｏｎｅｙ）のパターン認識により、スパムメールと判断しない場合は、これを破棄し、以後の処理を行わないオプションである。

【0036】

次に、スパムラベル管理サーバ３０は、スパム処理サーバ１０からＵＲＩスパムリスト１５１を取得するラベル取得部３１と、ＵＲＩのリソースを取得し，これを人が読める形で表示し，当該ＵＲＩのリソースが有害か否か確認させ，その結果を確定するラベル確定部３２と、確定したＵＲＩをスパム処理サーバ１０のスパムラベル保存部１５に保存するためのラベル保存部３３とから構成されている。

【0037】

ここで、スパムラベル管理サーバ３０はスパム処理サーバ１０によるスパムメール受付と同時に動作してもよいし、後日、スパムラベル管理サーバ３０の操作者によって動作してもよい。

【0038】

フィルタリングエンジン２０は、あらかじめＵＲＩスパムリストによってフィルタリングを行うか否かを含めて設定が可能なフィルタ設定管理部２１と、リソース閲覧用クライアント０４からＵＲＩ参照要求の際にスパム処理サーバ１０からＵＲＩスパムリスト１５１を取得するためのスパムラベル取得部２２と、ＵＲＩスパムリスト１５１をキャッシュとして保存したスパムラベルキャッシュ部２６と、それを管理するキャッシュ管理部２５と、フィルタ設定管理部２１が設定した状態およびスパムラベル取得部２２が取得したＵＲＩスパムリストによってフィルタリングを行うフィルタリング処理部２４と、フィルタリング不要の場合に当該ＵＲＩのリソースを取得するリソース取得部２３とから構成されている。

【0039】

ここで、スパムラベルキャッシュ部２６はスパムラベル取得部２２が取得したＵＲＩスパムリスト１５１を保存してもよいし、閲覧可能か否かという情報のみ、あるいはＵＲＩスパムリスト１５１を識別する加工値（ハッシュなど）であってもよい。

【0040】

図１において、スパム受付用メールアドレス０２１は、スパム処理サーバ１０が受け付ける専用のメールアドレスであり、任意のＷｅｂサイト０２に掲載しておく。スパム発行端末０３はＷｅｂサイト０２に掲載されたスパム受付用メールアドレス０２１を収集エンジンを使って収集し、収集したメールアドレスに対して大量のスパムメールを発行する。

【0041】

スパム処理サーバ１０は、スパム受付部１１において発行されたスパムメールを受信し

、その内容を解析処理部１２において解析してスパムメール内に含まれるＷｅｂサイトのリソースを指すＵＲＩを抽出し、それをＵＲＩスパムリスト１５１としてスパムラベル保存部１５にスパムリスト登録部１３が登録を行う。

【0042】

上記の登録処理とは非同期に、スパムラベル管理サーバ３０においては、スパム処理サーバ１０が自動で保存したスパムラベル保存部１５のＵＲＩスパムリスト１５１に誤りがないかを確認し、補正するために、ラベル取得部３１がスパム処理サーバ１０のスパムラベル応答部１４を介してＵＲＩスパムリスト１５１を取得する。

【0043】

さらに、ラベル確定部３２において、このＵＲＩが指すリソースを取得し、この内容を人が目視確認することにより、有害か否かの判断を行い、その結果によりラベル保存部３３がスパム処理サーバ１０のスパムリスト登録部１３を介して、スパムラベル保存部１５のＵＲＩスパムリスト１５１について、削除などの更新を行う。

【0044】

一方、リソース閲覧用クライアント０４からフィルタリンクエンジン２０を通してＵＲＩのリソースを閲覧する場合、あらかじめフィルタ設定管理部２１によりスパムメールをフィルタリングする設定にしておく。フィルタリングエンジン２０においては、リソース閲覧用クライアント０４からの要求により参照しようとしているＵＲＩがスパムリストに登録されていないかを調べるため、スパムラベル取得部２２がスパム処理サーバ１０のスパムラベル応答部１４からＵＲＩスパムリスト１５１を取得するか、あるいはＵＲＩスパムリスト１５１に登録されているかいないかという情報のみを取得する。

【0045】

続いて、フィルタリング処理部２４によっては、当該ＵＲＩがＵＲＩスパムリスト１５１に登録されていると判断した場合は、リソース閲覧用クライアント０４に当該ＵＲＩの閲覧はできない旨を返却し、あるいはＵＲＩスパムリスト１５１に登録されていないと判断した場合は、当該ＵＲＩのリソースをリソース取得部２３によって取得し、これをリソース閲覧用クライアント０４に送付する。

【0046】

ここで、スパム処理サーバ１０のスパムラベル応答部１４から取得したＵＲＩスパムリスト１５１の情報はキャッシュ管理部２５とスパムラベルキャッシュ部２６により保存され、次回のフィルタリング処理部２４によるＵＲＩ閲覧可否判断の際に、スパム処理サーバ１０への問い合わせを行わないようキャッシュ処理することも可能である。

【0047】

図２は上記のスパムメールフィルタリングシステムにおけるスパムメール受付動作を示す流れ図である。

【0048】

まず、スパム発行端末０３はＷｅｂサイト０２にある不特定多数のメールアドレスを収集エンジンなどを使って収集し、収集したメールアドレスに対して大量のスパムメールを発行する。ここで、Ｗｅｂサイト０２に登録されたスパム受付用メールアドレス０２１も収集され、スパム発行端末０３はスパム受付用メールアドレス０２１にもスパムメールを発行する（Ｆ０１）。

【0049】

スパム処理サーバ１０ではスパム受付用メールアドレス０２１の受信をスパム受付部１１が行っており、スパムメールの受信を行う（Ｆ０２）。

【0050】

続いて、受信したスパムメールの内容を解析し、メール内に含まれるＵＲＩを抽出する（Ｆ０３）。

【0051】

ここで、当該スパムメールにＵＲＩが含まれない場合は、そのまま当該スパムメールは破棄される。抽出したＵＲＩは、スパムリスト登録部１３によってスパムラベル保存部１

５のＵＲＩスパムリスト１５１へ登録される（Ｆ０４）。

【0052】

ここまでは自動的に処理されるものであるが、ＵＲＩスパムリスト１５１に登録されたＵＲＩが、本当にフィルタリングすべき情報か否かを確認することもできるべきである。

【0053】

そのため、スパムラベル管理サーバ３０においては、ラベル取得部３１によってスパム処理サーバ１０のＵＲＩスパムリスト１５１の要求を行い（Ｆ０５）、スパム処理サーバ１０のスパムラベル応答部１４がＵＲＩスパムリスト１５１を返却し（Ｆ０６）、このＵＲＩスパムリスト１５１から１つずつＵＲＩが指すＷｅｂサイトのリソースを参照し（Ｆ０７）、これを人が読める形で表示し、当該ＵＲＩのリソースが有害か否か目視確認させ、ラベル確定部３２においてその結果を確定し（Ｆ０８）、ラベル保存部３３によってそのＵＲＩをスパム処理サーバ１０に更新依頼する（Ｆ０９）。

【0054】

スパム処理サーバ１０はこの更新依頼によって、確定したＵＲＩスパムリスト１５１の更新を行う（Ｆ１０）。ここで更新とは、当該ＵＲＩをＵＲＩスパムリスト１５１から削除すること、あるいはＵＲＩスパムリスト１５１にある当該ＵＲＩに無効フラグを付加するなどによって更新することを含む。

【0055】

図３は上記のスパムメールフィルタリングシステムにおけるフィルタリング動作を示す流れ図である。

【0056】

管理者（この場合、たとえば子供にスパムメールに含まれるＷｅｂリソースを閲覧させたくないと考える親である場合、あるいは社員が業務時間中に業務に関係ないスパムメールに含まれるＷｅｂリソースを閲覧させたくない上司など）は、まずフィルタリングエンジン２０にスパムメールに含まれるＵＲＩをフィルタリングするための設定を、リソース閲覧用クライアント０４からフィルタリングエンジン２０に行っておく。あるいはリソース閲覧用クライアント０４ではなく、フィルタリングエンジン２０に管理者が直接設定してもよい（Ｆ２１，Ｆ２２）。

【0057】

設定の内容は、スパムメールに含まれるＵＲＩ参照のフィルタリングを行うか否かという設定や、利用者に応じた設定（たとえば子供がリソース閲覧用クライアント０４を使う場合フィルタするが、親が使う場合フィルタしないなど）でもよい。

【0058】

次に、情報閲覧者（この場合、たとえば子供や社員など）は、インターネットなどのネットワーク０１上にあるＷｅｂサイト０２のＷｅｂページや音楽、映像などＷｅｂリソースなどの情報であるリソースを、リソース閲覧用クライアント０４を使い、フィルタリングエンジン２０を介して、要求する（Ｆ２３）。

【0059】

所望のＵＲＩのリソースを閲覧あるいは取得する場合、スパムラベル取得部２２は、フィルタリングエンジン２０の高速化のために、過去に使われた同じＵＲＩがＵＲＩスパムリストとしてスパムラベルキャッシュ部２６に登録されていれば、キャッシュ管理部２５を介して参照し（Ｆ２４）、キャッシュに存在しない場合は、スパム処理サーバ１０のスパムラベル応答部１４からスパムラベル保存部１５のＵＲＩスパムリスト１５１を入手する（Ｆ２５，Ｆ２６）。

【0060】

ここで、ＵＲＩスパムリスト１５１はスパムメールに含まれていたＵＲＩか否かを判断するためのものであり、スパムメールに含まれていた実際のＵＲＩのリストでもよいし、ＵＲＩスパムリスト１５１を識別する加工値（ハッシュなど）であってもよい。

【0061】

次に、フィルタリング処理部２４は、当該ＵＲＩがＵＲＩスパムリスト１５１に存在す

るか否かによってフィルタリングするか否かを判断し（Ｆ２７）、フィルタリングすると判断した場合は、フィルタリングされたために閲覧できない旨のメッセージをリソース閲覧用クライアント０４に返す（Ｆ２８）。

【0062】

フィルタリングの必要がないと判断した場合は、ＵＲＩが指すＷｅｂサイトのリソースをリソース取得部２３によって取得し（Ｆ２９）、これをリソース閲覧用クライアント０４に返す（Ｆ３０）。

【0063】

リソース閲覧用クライアント０４は、フィルタリングエンジン２０から返却されたフィルタリングされたために閲覧できない旨のメッセージか、あるいは当該ＵＲＩのリソースを、情報閲覧者に提示する（Ｆ３１）。

【0064】

図４は本発明の実施の第二の形態を示す構成図である。同図において、スパムメールフィルタリングシステムは、あらかじめ関連するキーワード１７１を登録しているキーワード保存部１７と、スパムメールを解析する際にそれに含まれるキーワードもＵＲＩとともに抽出する解析処理部１２ａと、前記キーワードを登録されているものと比較しその有害度を格付けるスパムラベル格付部１６と、この格付結果に基づいて当該ＵＲＩ１５２およびスパムラベル１５３をスパムラベル保存部１５ａに登録するスパムラベル登録部１８とを備えるスパム処理サーバ１０ａを有している。

【0065】

なお、図４において、上記スパム処理サーバ１０ａ以外の各構成ブロックは、図１において既述したスパムメールフィルタリングシステムと同一の機能構成を備えている。

【0066】

図５は、図４に示したスパムメールフィルタリングシステムのスパムメール受付動作を示す流れ図である。

【0067】

最初に、スパムメールが発行され（Ｆ４１）、これを受信する（Ｆ４２）までは同じであるが、スパム処理サーバ１０ａのスパム受付部１１が受け付けたスパムメールを解析処理部１２ａにおいて解析する際に、ＵＲＩのほかにスパムメールに含まれるキーワードまで抽出を行い、スパムラベル格付部１６が、抽出したキーワードとあらかじめ登録されているキーワード保存部１７のキーワード１７１を比較することにより、当該キーワードの有害度を判断する（Ｆ４３，Ｆ４４）。たとえば、有害なキーワードが含まれているほど、当該ＵＲＩは有害であるとする。

【0068】

ここで、スパムメールからキーワードを抽出する方法は、スパムメールのヘッダ（発行者，あて先，経由など）に含まれる文字からキーワード抽出する場合や、スパムメール本体に含まれる本文からキーワードを抽出する場合のほか、スパムメール内のＵＲＩに含まれる文字列からキーワードを抽出する場合などがある。また、スパムラベル格付部１６がキーワードを比較する方法は、文字列の完全一致や、あいまい検索（正規化表現）などを含む。

【0069】

次に、スパムラベル登録部１８では、スパムラベル格付部１６の格付結果により、当該ＵＲＩ（ＵＲＩ１５２）とその格付値（スパムラベル１５３）をスパムラベル保存部１５ａに登録する（Ｆ４５）。

【0070】

ここまでは自動的に処理されるが、登録されたＵＲＩが、本当にフィルタリングすべき情報か否かを確認することもできるべきであることは、既述の通りである。

【0071】

すなわち、スパムラベル管理サーバ３０においては、ラベル取得部３１によってスパム処理サーバ１０ａにＵＲＩ１５２およびスパムラベル１５３の要求を行い（Ｆ４６）、ス

パム処理サーバ１０ａのスパムラベル応答部１４がそれらを返却する（Ｆ４７）。

【0072】

このＵＲＩ１５２をもとにＵＲＩが指すＷｅｂサイトのリソースを参照し（Ｆ４８）、これを人が読める形で表示し、当該ＵＲＩのリソースが有害か否か目視確認させ、ラベル確定部３２においてその結果を確定し（Ｆ４９）、確定したＵＲＩをラベル保存部３３によってスパム処理サーバ１０ａに更新依頼を行う（Ｆ５０）。

【0073】

スパム処理サーバ１０ａはこの更新依頼によって、確定したＵＲＩおよびスパムラベルにより更新を行う（Ｆ５１）。ここで更新とは、当該ＵＲＩをＵＲＩスパムリストから削除すること、あるいはＵＲＩスパムリストにある当該ＵＲＩに無効フラグを付加するなどによって更新すること、あるいは当該ＵＲＩ１５２のスパムラベル１５３に入る格付値の変更を含む。

【0074】

なお、リソース閲覧時のフィルタリング動作は既述の通りである（図３参照）。

【0075】

図６は本発明の実施の第三の形態を示す構成図である。同図におけるスパムメールフィルタリングシステムは、スパム受信用のメールアドレスを専用に用意することができない場合で、複数の有効なメールアドレスを用意できる場合、スパムメールは同じ内容を複数のメールアドレスに配送する特徴があることを利用している。

【0076】

すなわち、図６において、Ｗｅｂサイト０２には新たにスパムメール受付用メールアドレスＢ０２２が追加され、このアドレス宛のメールはスパム受付部Ｂ４１を備えるスパム処理サーバＢ４０で受け付けられた後、スパム処理サーバ１０ｂに送付される。

【0077】

スパム処理サーバ１０ｂは、スパム受付用メールアドレス０２１宛のメールを受け付けて解析すると共に、スパム処理サーバＢ４０から送付されたメールも解析処理し、二重受付をチェックする解析処理部１２ｂを備える。

【0078】

ここで、スパム受付用メールアドレス０２１とスパム受付用メールアドレスＢ０２２とは同じＷｅｂサイト０２にあってもよし、異なるＷｅｂサイトにあっても、あるいは別のＷｅｂページにあってもよい。。さらに、スパム受付用メールアドレスＢ０２２、スパム処理サーバＢ４０は複数存在していてもよい。

【0079】

図７は、図６に示したスパムメールフィルタリングシステムのスパムメール受付動作を示す流れ図である。

【0080】

スパム発行端末０３は、Ｗｅｂサイト０２にある不特定多数のメールアドレスを収集エンジンなどを使って収集し、収集したメールアドレスに対して大量のスパムメールを発行する。その際、Ｗｅｂサイト０２またはその他のサイトに登録されたスパム受付用メールアドレスＢ０２２も収集され、スパム発行端末０３はスパム受付用メールアドレスＢ０２２にスパムメールを発行する（Ｆ６１）。

【0081】

スパム処理サーバＢ４０では、スパム受付用メールアドレスＢ０２２の受信をスパム受付部Ｂ４１が行っており、スパムメールの受信を行い、受信したメールをスパム処理サーバ１０ｂに渡す（Ｆ６２）。

【0082】

さらに、スパム発行端末０３は、同様のメールをスパム受付用メールアドレス０２１にも発行する（Ｆ６３）。

【0083】

スパム処理サーバ１０ｂでは、スパム受付用メールアドレス０２１の受信をスパム受付

部１１が行っており、スパムメールの受信を行う（Ｆ６４）。

【0084】

次に、解析処理部１２によって、受信したスパムメールの内容を解析するが、まず、スパム処理サーバＢ４０のスパム受付部Ｂ４１から渡されたスパムメールと同期を取るため、２つの同じ本文のメールの付き合わせ確認を行い、本文が同じメールがスパム処理サーバ１０ｂとスパム処理サーバＢ４０の２カ所で受信したことを確認すれば、その何れかのスパムメールについて、メール内に含まれるＵＲＩを抽出する（Ｆ６５）。

【0085】

ここで、当該スパムメールにＵＲＩが含まれない場合は、そのまま当該スパムメールは破棄される。

【0086】

また、２つの同じ本文のメールを把握する際にも、たとえば、メールアドレスの先頭部分のみを抽出したあて先を含むケースがあり（たとえば、ｕｅｄａ@ｗｅｂｐａｇｅ．ｏｒ．ｊｐであれば、ｕｅｄａ様へのご案内という本文を含むなど）、全く同じ本文か否かではなく、同じ内容を９０％以上含む本文であるという照合率による比較が、必要となる。

【0087】

ここで、９０％は例であり、設定は”@”文字を含むメールアドレス、あるいは「様へ」などのキーワードを用いることにより、メールの照合を行わない部分を指定するといった文字列指定も行うことが考えられる。

【0088】

また、スパム処理サーバ１０ｂとスパム処理サーバＢ４０が受信するスパムメールの順番はどちらのサーバが先でも、あるいは同時でもよく、それらのスパムメールを解析する解析処理部１２ｂでは、複数のスパムメールを保存するキューを用いることが有効な手段でもある。

【0089】

さらに、スパム処理サーバＢ４０に相当する機能を複数用意する場合は、それら全てのサーバがスパムメールを受信した場合に解析処理部１２ｂを起動するか、あるいは2つ以上、もしくは1つだけでも解析処理部１２ｂを起動するか特に規定しない。

【0090】

さて、抽出したＵＲＩはスパムリスト登録部１３によってスパムラベル保存部１５のＵＲＩスパムリスト１５１へ登録される（Ｆ６６）。

【0091】

ここまで自動的に処理されるものであるが、ＵＲＩスパムリスト１５１に登録されたＵＲＩが、本当にフィルタリングすべき情報か否かを確認することもできるべきである。

【0092】

すなわち、既述したように、スパムラベル管理サーバ３０を任意に操作し、ＵＲＩのリソースを目視確認することができる。図７において、Ｆ６７～Ｆ７２の処理は図２におけるＦ０５～Ｆ１０の処理と同じであるので、ここでは説明を繰返さない。

【0093】

なお、上記のスパムメールフィルタリングシステムにおいても、リソース閲覧時のフィルタリング動作は図３において説明した通りである。

【産業上の利用可能性】

【0094】

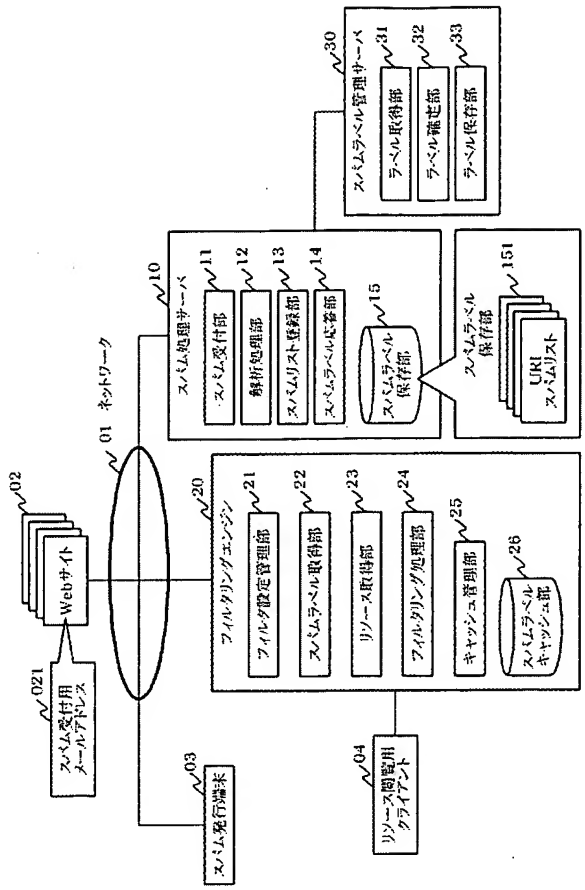
ＵＲＩなどのデータ収集を機械的に行っており、それをフィルタリングに即時反映することができる。また、ＵＲＩリソースの目視による確認チェックを行うことができるので、フィルタリングの品質を維持管理することが可能になる。したがって、情報管理部門にとって有用なフィルタリング手法を提供できる。

【図面の簡単な説明】

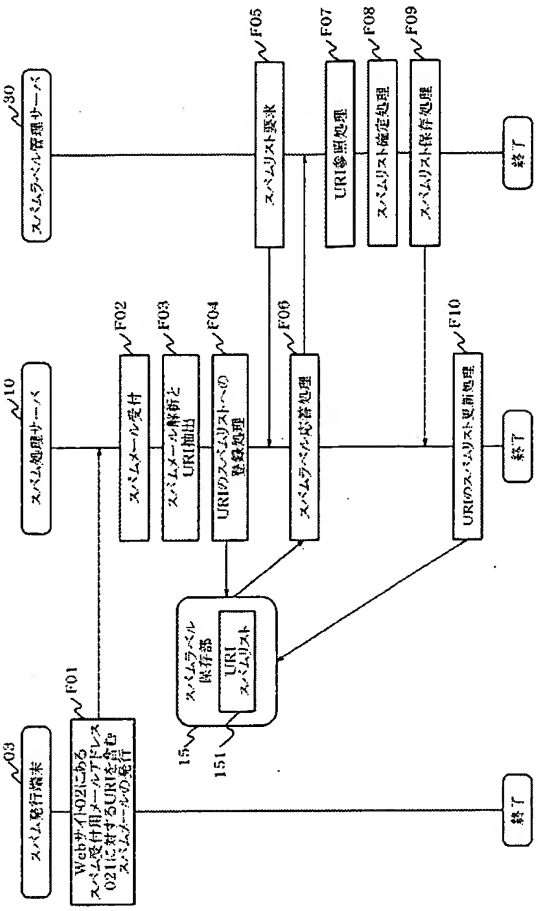
【0095】

【図1】本発明の実施の第一の形態を示す構成図。
【図2】スパムメールの受付動作を示す流れ図。
【図3】リソース閲覧時のフィルタリング動作を示す流れ図。
【図4】本発明の実施の第二の形態を示す構成図。
【図5】図４の実施例におけるスパムメール受付動作を示す流れ図。
【図6】本発明の実施の第三の形態を示す構成図。
【図7】図６の実施例におけるスパムメール受付動作を示す流れ図。
【符号の説明】
【0096】
０１　ネットワーク
０２　Ｗｅｂサイト
０２１　スパム受付用メールアドレス
０２２　スパム受付用メールアドレスＢ
０３　スパム発行端末
０４　リソース閲覧用クライアント
１０，１０ａ，１０ｂ　スパム処理サーバ
１１　スパム受付部
１２，１２ａ，１２ｂ　解析処理部
１３　スパムリスト登録部
１４　スパムラベル応答部
１５，１５ａ　スパムラベル保存部
１６　スパムラベル格付部
１７　キーワード保存部
１８　スパムラベル登録部
２０　フィルタリングエンジン
２１　フィルタ設定管理部
２２　スパムラベル取得部
２３　リソース取得部
２４　フィルタリング処理部
２５　キャッシュ管理部
２６　スパムラベルキャッシュ部
３０　スパムラベル管理サーバ
３１　ラベル取得部
３２　ラベル確定部
３３　ラベル保存部
４０　スパム処理サーバＢ
４１　スパム受付部Ｂ
１５１　ＵＲＩスパムリスト
１５２　ＵＲＩ
１５３　スパムラベル
１７１　キーワード

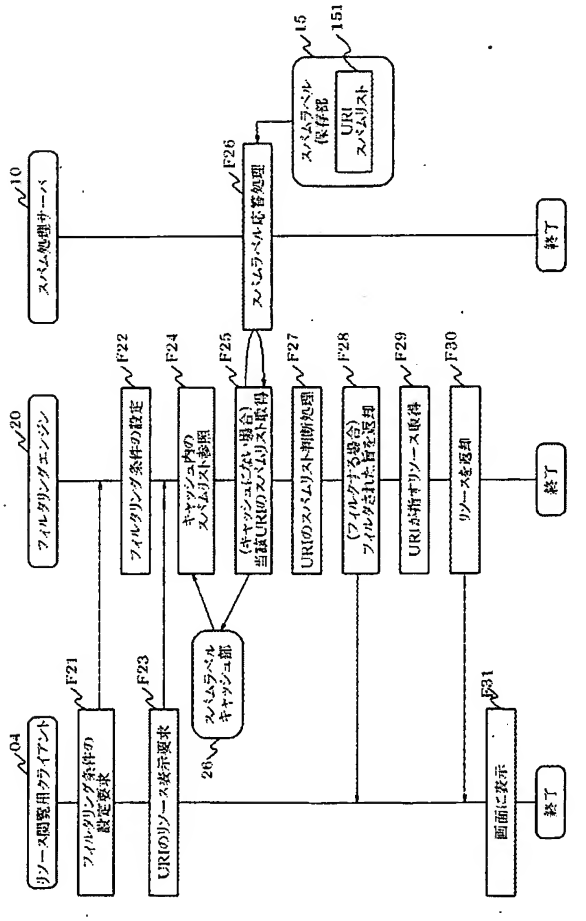
【図1】


01 ネットワーク
02
Webサイト
021
スパム受付用メールアドレス
03
スパム発行端末
04
リソース閲覧用クライアント
10
スパム処理サーバ
11
スパム受付部
12
解析処理部
13
スパムリスト登録部
14
スパムラベル応答部
15
スパムラベル保存部
151
URI スパムリスト
20
フィルタリングエンジン
21
フィルタ設定管理部
22
スパムラベル取得部
23
リソース取得部
24
フィルタリング処理部
25
キャッシュ管理部
26
スパムラベルキャッシュ部
30
スパムラベル管理サーバ
31
ラベル取得部
32
ラベル確定部
33
ラベル保存部

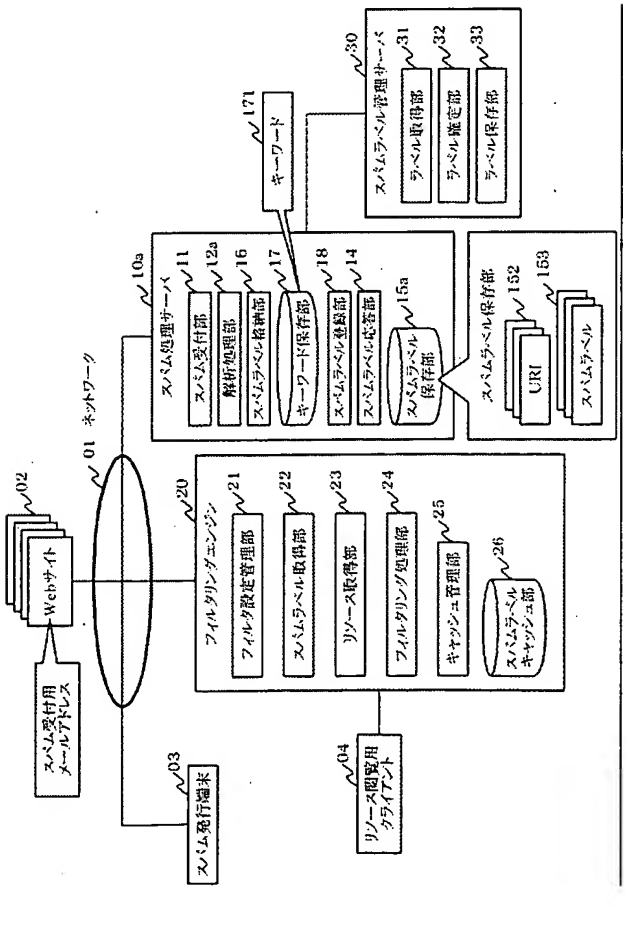
【図2】


30
スパムラベル管理サーバ
10
スパム処理サーバ
03
スパム発行端末
F01
Webサイト02にあるスパム受付用メールアドレス021に対するURIを含むスパムメールの発行
F02
スパムメール受付
F03
スパムメール解析とURI抽出
F04
URIのスパムリストへの登録処理
F05
スパムリスト要求
F06
スパムラベル応答処理
F07
URI参照処理
F08
スパムリスト確定処理
F09
スパムリスト保存処理
F10
URIのスパムリスト更新処理
15
151
スパムラベル保存部
URI スパムリスト
終了

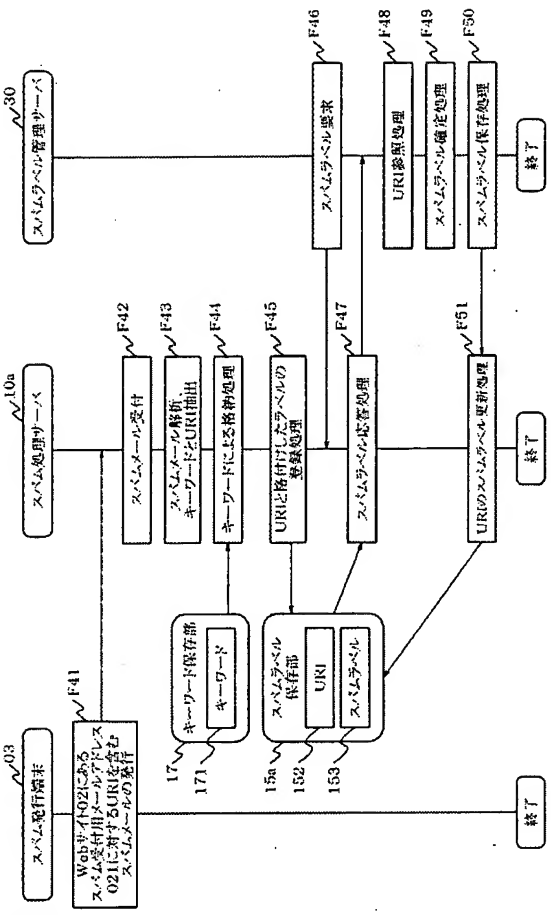
【図3】


04
リソース閲覧用クライアント
F21
フィルタリング条件の設定要求
F23
URIのリソース表示要求
20
フィルタリングエンジン
F22
フィルタリング条件の設定
F24
キャッシュ内のスパムリスト参照
F25
(キャッシュにない場合)当該URIのスパムリスト取得
26
スパムラベルキャッシュ部
10
スパム処理サーバ
F26
スパムラベル応答処理
15
151
スパムラベル保存部
URI スパムリスト
F27
URIのスパムリスト判断処理
F28
(フィルタされる場合)フィルタされた旨を返却
F29
URIが指すリソース取得
F30
リソースを返却
F31
画面に表示
終了
終了
終了

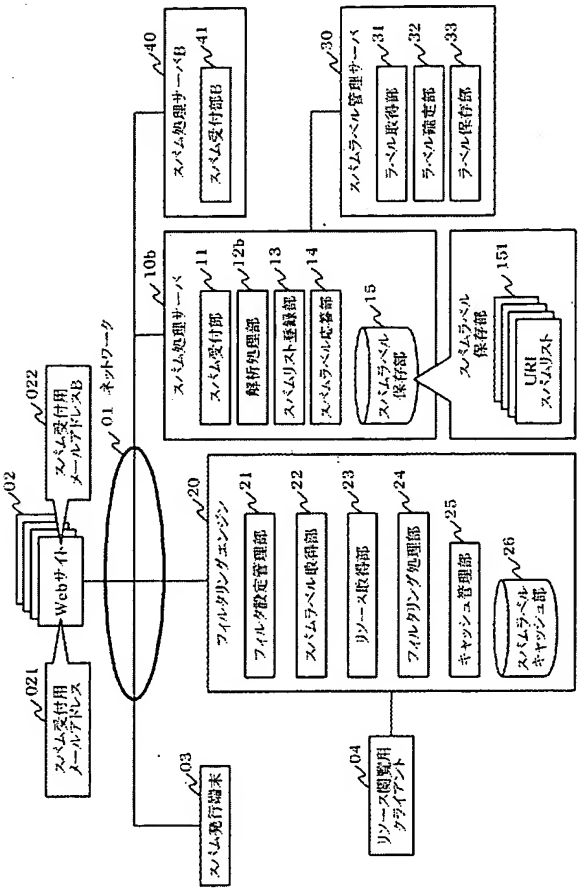
【図4】


01 ネットワーク
02
Webサイト
021
スパム受付用メールアドレス
03
スパム発行端末
04
リソース閲覧用クライアント
10a
スパム処理サーバ
11
スパム受付部
12a
解析処理部
16
スパムラベル格納部
17
キーワード保存部
18
スパムラベル登録部
14
スパムラベル応答部
15a
スパムラベル保存部
171
キーワード
20
フィルタリングエンジン
21
フィルタ設定管理部
22
スパムラベル取得部
23
リソース取得部
24
フィルタリング処理部
25
キャッシュ管理部
26
スパムラベルキャッシュ部
30
スパムラベル管理サーバ
31
ラベル取得部
32
ラベル確定部
33
ラベル保存部
152
URI
153
スパムラベル

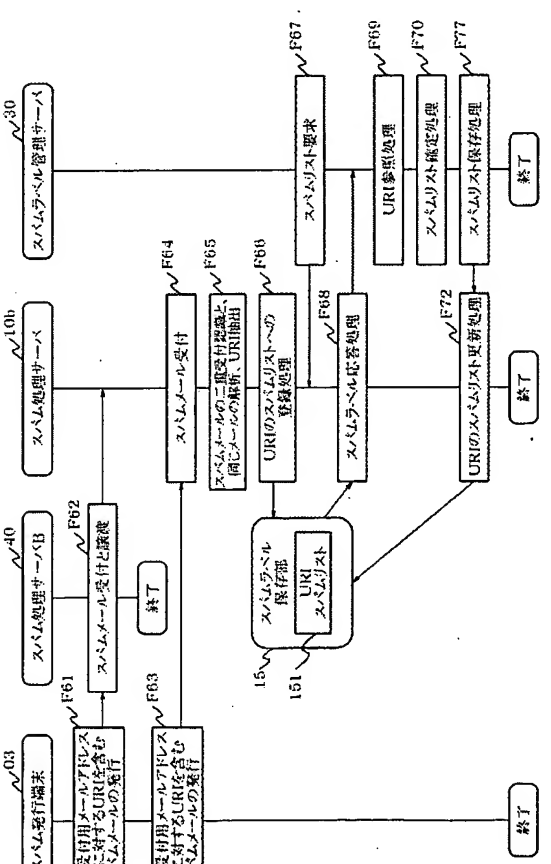
【図5】


スパム発行端末
スパム処理サーバ
スパムラベル管理サーバ
Webサイト02にあるスパム受付用メールアドレス021に対するURIを含むスパムメールの発行
スパムメール受付
スパムメール解析、キーワードとURI抽出
キーワードによる格納処理
URIと格付けしたラベルの登録処理
スパムラベル要求
スパムラベル確定処理
スパムラベル保存処理
URI参照処理
スパムラベル応答処理
URIのスパムラベル更新処理
キーワード保存部
スパムラベル保存部
終了

【図6】


スパム受付用メールアドレス
Webサイト
ネットワーク
スパム処理サーバ
スパム受付部
解析処理部
スパムリスト登録部
スパムラベル応答部
スパムラベル保存部
スパム処理サーバB
スパム受付部B
スパムラベル管理サーバ
ラベル取得部
ラベル確定部
ラベル保存部
ファイルタリングエンジン
フィルタ設定管理部
スパムラベル収得部
リソース取得部
フィルタリング処理部
キャッシュ管理部
スパムラベルキャッシュ部
URIスパムリスト
リソース閲覧用ブラウザイアント
スパム発行端末

【図7】


スパム発行端末
スパム処理サーバ
スパムラベル管理サーバ
スパム受付用メールアドレス022に対するURIを含むスパムメールの発行
スパム受付用メールアドレス021に対するURIを含むスパムメールの発行
スパムメール受付と識別
スパムメール受付
スパムメールの二重受付記録と同じメールの解析、URI抽出
URIのスパムリスト への登録処理
スパムラベル応答処理
スパムリスト要求
URI参照処理
スパムリスト確定処理
スパムリスト保存処理
URIのスパムリスト更新処理
スパムラベル保存部
URI
スパムリスト
終了

【要約の続き】